عدم توجه به نصب وصله‌ها

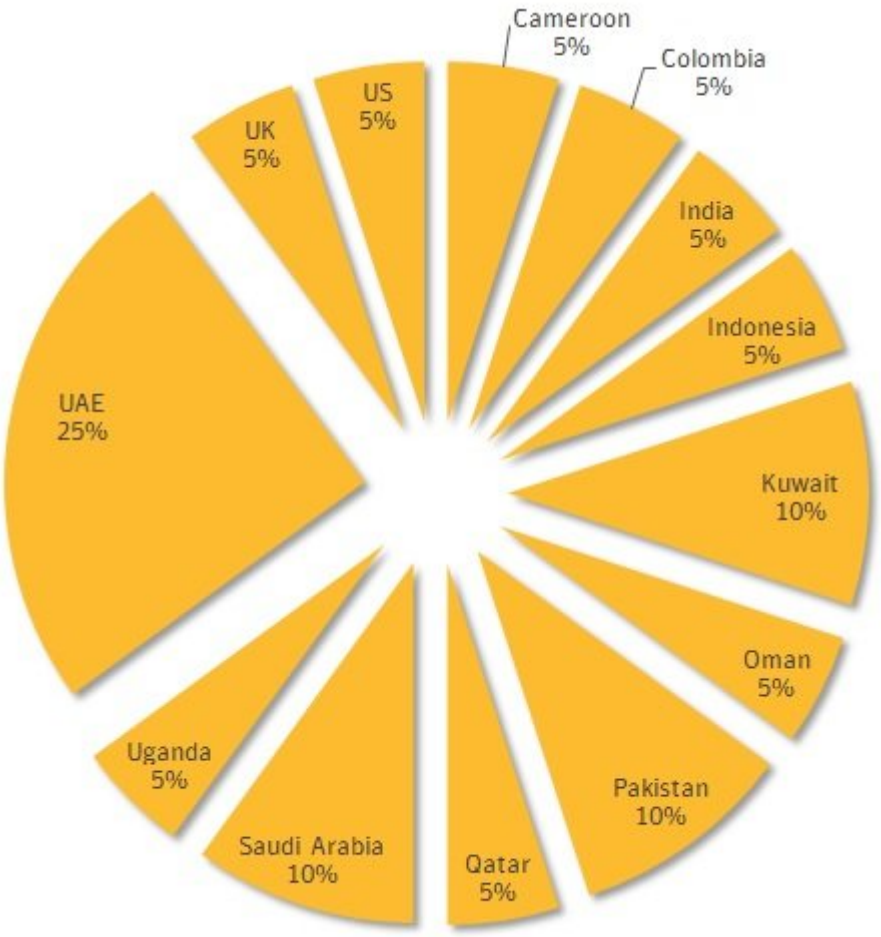
حمله یک تروجان به شرکت‌های حامل انرژی

در ماه‌های ژانویه و فوریه امسال، تیم تحقیقاتی سیمانتک موفق به شناسایی یک کمپین حمله که هدف آن شرکت‌های انرژی در سرتاسر جهان بود، شدند. کانون توجه این حمله خاورمیانه است. این کمپین حمله، با هدف سرقت اطلاعات طراحی شده است. سیمانتک نام بدافزاری که در این حمله شرکت دارد را تروجان Laziok نام‌گذاری کرده است. Laziok در قالب یک ابزار شناسایی، توانایی جمع‌آوری اطلاعات در مورد کامپیوتر در معرض خطر را فراهم می‌کند.

محققان امنیتی به تازگی خبر از یک کمپین جاسوسی داده‌اند که از یک بدافزار سفارشی طراحی شده برای دسترسی به اطلاعات محرمانه شرکت‌های حامل انرژی در سرتاسر جهان استفاده می‌کند. در یادداشتی که توسط تیم تحقیقاتی سیمانتک منتشر شده است؛ این شرکت امنیتی اعلام کرد؛ Trojan.Laziok بدافزاری است که برای شناسایی کامپیوترهای آلوده و دریافت داده‌هایی از قبیل نام ماشین، نرم‌افزارهای نصب شده، میزان حافظه اصلی، اندازه هارددیسک، جزییات پردازشگر مرکزی، جزییات پردازشگر گرافیکی و نرم‌افزار ضدویروس نصب شده، سیستم قربانی را مورد جستجو قرار می‌دهد.

حمله‌کننده‌ها از این اطلاعات برای نحوه آلوده‌سازی یک کامپیوتر با نسخه‌های دیگری از این بدافزار همچون Backdoor.Cyberat و Trojan.Zbot استفاده می‌کنند. این بدافزارها به طور ویژه برای در معرض خطر قرار دادن یک کامپیوتر طراحی شده‌اند. کریستین تیریپوتی، محقق سیسمانتک می‌گوید: «اطلاعات جزیی‌تر به هکرها این توانایی را می‌دهد که تصمیم‌گیری‌های مهم‌تری درباره این‌که چگونه حمله خود را پیش برده یا آن‌را متوقف کنند، ارائه دهند. در مدت زمانی که ما در حال پژوهش روی این بدافزار بودیم، کشف کردیم که اکثر قریب به اتفاق اهدافی که این بدافزار روی آن‌ها متمرکز است، در ارتباط با صنایع نفت و گاز و هلیوم قرار دارند. هر شخص یا گروهی که در پشت این حملات قرار دارند، ممکن است به منافع راهبردی شرکت‌هایی که آن‌ها را آلوده ساخته‌اند، علاقه مند باشد.»

تصویر زیر مناطقی که هدف این بدافزار بوده است را نشان می‌دهد.



امارات متحده عربی اصلی‌ترین هدف هکرها و در ادامه کشورهای عربستان، پاکستان و کویت قرار دارند. کامپیوترها با ارسال هرزنامه نامه‌ای که از دامنه moneytrans[.]eu ارسال می‌شود، به بدافزار Lazoiok آلوده می‌شوند. ایمیل‌های آلوده شامل یک ضمیمه آلوده اکسپلویت بوده که از یک آسیب‌پذیری ویندوز مایکروسافت که وصله آن در سال 2012 منتشر شد، استفاده می‌کند. این آسیب‌پذیری در موارد مشابهی همچون Red October که برای آلوده‌سازی دیپلماتیک، دولتی و سازمان‌های علمی در حداقل 39 کشور جهان مورد استفاده قرار گرفته بود، استفاده می‌کند. اکسپلویت Laziok عمدتا در قالب یک فایل اکسل ارسال می‌شود. زمانی‌که کاربر اقدام به باز کردن این ضمیمه آلوده کند؛ کدهای اکسپلویت اجرا می‌شوند. اگر اکسپلویت موفقیت آمیز باشد، تروجان Lazoik آزاد شده و اقدام به آلوده‌سازی سیستم قربانی می‌کند. این تروجان خودش را در پوشه زیر پنهان می‌کند.

SystemDrive%\Documents and Settings\All Users\Application Data\System\Oracle%

بعد از آلوده‌سازی سیستم، تروجان پوشه‌های دیگری ساخته و خودش را با نام‌های مختلف درون این پوشه‌ها قرار می‌دهد.

•%SystemDrive%\Documents and Settings\All Users\Application Data\System\Oracle\azioklmpx\search.exe

•%SystemDrive%\Documents and Settings\All Users\Application Data\System\Oracle\azioklmpx\ati.exe

•%SystemDrive%\Documents and Settings\All Users\Application Data\System\Oracle\azioklmpx\lsass.exe

•%SystemDrive%\Documents and Settings\All Users\Application Data\System\Oracle\azioklmpx\smss.exe

•%SystemDrive%\Documents and Settings\All Users\Application Data\System\Oracle\azioklmpx\admin.exe

•%SystemDrive%\Documents and Settings\All Users\Application Data\System\Oracle\azioklmpx\key.exe

•%SystemDrive%\Documents and Settings\All Users\Application Data\System\Oracle\azioklmpx\taskmgr.exe

•%SystemDrive%\Documents and Settings\All Users\Application Data\System\Oracle\azioklmpx\chrome.exe

البته به نظر می‌رسد، گروهی که در پشت این حمله قرار دارند یک گروه پیشرفته نیستند، به دلیل این‌که آن‌ها از یک آسیب‌پذیری قدیمی برای انتشار تهدیدات خود استفاده کرده‌اند. با این حال، هنوز هم بسیاری از مردم اقدام به نصب وصله ارائه شده برای این آسیب‌پذیری که سال‌ها از عمر آن می‌گذرد نکرده و خودشان را در معرض حملاتی از این نوع قرار می‌دهند. از دید هکرها، آن‌ها نیازی به استفاده از جدیدترین ابزارها برای موفقیت در کارهای‌شان ندارند، همه آن چیزی که هکرها به آن نیاز دارند کمی اطلاعات از فعالیت‌های امنیتی کاربر و آگاهی از عدم نصب وصله‌ها است.

تاریخ انتشار:
19 فروردین 1394

نشانی منبع: https://www.shabakeh-mag.com/news/world/498